Chronicle SIEM Fundamentals (CSIEMF)

ID CSIEMF **Price** 2,396.— €(excl. tax) **Duration** 3 days

Who should attend

Individuals who need a basic introduction to Chronicle SIEM

Prerequisites

Basic knowledge about what is SIEM & SOAR

Course Objectives

Explore the essentials of Chronicle, a powerful Security Information and Event Management (SIEM) solution offered as a cloud service on the robust Google infrastructure. The Chronicle Fundamentals course provides an in-depth overview of the key functionalities, data analysis capabilities, and security aspects of Chronicle SIEM.

- Chronicle Access – Role-Based Access Control (RBAC) in Chronicle. Why Audit logging is important and how to implement it in your Chronicle instance.
- Learn about Raw Log Search and UDM Search, how to use Search for investigation.
- Chronicle Data On Boarding: forwarders, feed management, ingestion API, and direct ingestion.
- Introduction to Chronicle Parsers – What is a parser, versioning, and parser extension.
- Walkthrough of Chronicle Curated Detection rules.
- Navigating Alerts using the Alert Graph: Entity data, releted alerts, alert context.
- Learn about Entity data – Data enrichment in Chronicle, Entity types (Users & Assets), Resources, Geo IP Enrichment.
- Advanced Search Capabilities: Reference Lists, Group Fields, Pivot, Search for Alerts.
- Parsing data in Chronicle – What are parsers and how can we manage them: Parser update, versioning, parser extensions.
- Building rules for Chronicle: YARA-L 2.0 syntax, Rules UI, Single event rules, Multi-event rules, using entity data in rules, Outcomes, Functions & Lists, best practice.
- Building dashboards in Chronicle.

Course Content

- Module 1: Chronicle Access
- Module 2: Searching with Chronicle
  Hands-On: Raw Log & UDM Search
- Module 3: Chronicle Data On Boarding
  Hands-On: Collect Linux Syslog
- Module 4: Parsing Data In Chronicle
- Module 5: Curated Detections
- Module 6: Visualizing Alerts With Chronicle
  Hands-On: Navigating and Reviewing using Alert Graph
- Module 7: Entity Graph
  Hands-On: Search – Asset\User Enrichment
- Module 8: Advance Searching With Chronicle
  Hands-On: Advanced Search
- Module 9: Building Rules For Chronicle
  Hands-On: Building Rules
- Module 10: Visualizing Alerts (Advance)
- Module 11: Entity Graph (Advance)
- Module 12: Visualizing Data in Chronicle Hands-On: Building Dashboard In Chronicle

About Fast Lane

Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.

Fast Lane Services

- ✓ High End Technology Training
- ✓ Business & Soft Skill Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digital Learning Solutions
- ✓ Content Development
- ✓ Remote Labs
- ✓ Talent Programs
- ✓ Event Management Services

Training Methods

- ✓ Classroom Training
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Classroom & Online Hybrid
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobile Learning

Technologies & Solutions

- ✓ Digital Transformation
- ✓ Artificial Intelligence
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Worldwide Presence
with high-end training centers around the globe

Multiple Awards
from vendors such as AWS, Microsoft, Cisco, Google, NetApp, VMware

Experienced SMEs
with over 19.000 combined certifications

Germany
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Austria
ITLS GmbH
(Partner of Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Switzerland
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch